The FDIC's Implementation of Supply Chain Risk Management

March 2022 **EVAL-22-003**

Evaluation Report

Audits, Evaluations, and Cyber

☆☆☆☆☆☆☆☆

NOTICE

On June 1, 2022, the Office of Inspector General made minor changes to page 15 of the report to correct the dates the FDIC issued two Procurement Administrative Bulletins. This correction did not affect the report's findings, conclusions, or recommendations.

Office of Inspector General

Executive Summary

The FDIC's Implementation of Supply Chain Risk Management

The FDIC utilizes numerous contract vehicles to support its operations and accomplish its mission. In 2021, the FDIC awarded 483 contracts totaling over $2 billion for the acquisition of products and services. These products and services are provided by many types of vendors, contractors, and subcontractors. The supply chain for each vendor, contractor, or subcontractor may present unique risks to the FDIC, including the installation of counterfeit hardware and software in the FDIC environment, or reliance on a malicious or unqualified provider. Further, the Agency may have reduced visibility, understanding, and control of these risks when its vendors rely on second- and third-tier suppliers and service providers.

Because the FDIC is a financial regulator and holds vast amounts of sensitive and nonpublic information, adversaries may seek to disrupt the Agency's operations, programs, and functions and may manipulate or exploit the sensitive information for their own purpose or benefit. According to the National Institute for Standards and Technology, "adversaries are using the supply chain as an attack vector and [as an] effective means of penetrating [United States' public and private] systems, compromising the integrity of system elements, and gaining access to critical assets." Therefore, the FDIC must implement a robust Supply Chain Risk Management (SCRM) Program to identify and mitigate supply chain risks that threaten its ability to fulfill its mission, goals, and objectives; protect its sensitive and nonpublic information; and maintain the integrity of its operations.

Our evaluation objective was to determine whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's objectives and best practices.

Results

The FDIC has not implemented several objectives outlined in its SCRM Implementation Project Charter (November 2019) and is not conducting supply chain risk assessments in accordance with best practices. In addition, the FDIC has not ensured that its Enterprise Risk Management (ERM) processes fully capture supply chain risks. Further, FDIC Contracting Officers did not maintain contract documents in the Contract Electronic File (CEFile) system, as required.

In relation to its SCRM Program, we found that the FDIC has not implemented several objectives established in the SCRM Implementation Project Charter. Specifically, the FDIC has not:

- Identified and documented known risks to the FDIC's supply chain;
- Defined a risk management framework to evaluate risks to non-Information Technology (IT) procurements; and
- Established metrics and indicators related to continuous monitoring and evaluation of supply chain risks.

The FDIC should continue its efforts to fulfill these SCRM Implementation Project Charter objectives to identify, evaluate, and monitor supply chain risks. Otherwise, it may be exposed to SCRM threats such as the use of counterfeit components or installation of malicious code. These threats could compromise the FDIC's IT and the data on its information systems and provide adversaries a means to exfiltrate sensitive information such as confidential bank examination information. Further, if the FDIC does not effectively monitor and evaluate supply chain risks, disruptions to the FDIC's supply chain could compromise the products, services, and facilities that enable the FDIC to perform its mission.

We also found that the FDIC is not conducting supply chain risk assessments during its procurement process for Chief Information Officer Organization and other Division and Office contracts. Risk assessments provide visibility into supply chain risks, which is important for identifying and monitoring potential vulnerabilities in FDIC procurements. Without increased visibility into the FDIC's supply chains and the associated risks, it is difficult for the FDIC to manage these risks and reduce their susceptibility to threats such as the installation of a backdoor into network monitoring software.

In addition, we found that the FDIC has not integrated Agency-wide supply chain risks into its ERM processes. While the FDIC has identified certain IT risks in its ERM Risk Inventory, the FDIC has not employed Agency-wide consideration of supply chain risk. As a result, the FDIC's Risk Inventory does not capture certain supply chain risks that FDIC Divisions and Offices face, nor does it capture supply chain risks associated with its non-IT products and services.

During the course of our evaluation, we also determined that Contracting Officers did not maintain contract documents in CEFile, as required. Not having critical documents in CEFile could lead to difficulty in enforcing a contract in the event of contractor noncompliance.

Recommendations

This report contains nine recommendations to improve the FDIC's SCRM Program and retention of contract documents. Specifically, we recommended that the FDIC identify, document, and monitor supply chain risks and conduct supply chain risk assessments of suppliers and vendors. We also recommended that the FDIC's Enterprise Risk Management Program articulate the extent and significance of supply chain risks. Lastly, we recommended an improvement to the FDIC's efforts to maintain contract documents in its filing system.

The FDIC concurred with all nine recommendations in this report. The FDIC plans to complete corrective action by November 30, 2022.

Contents

March 1, 2022

Subject | ***The FDIC's Implementation of Supply Chain Risk Management***

The FDIC utilizes numerous contracting vehicles to support its operations and accomplish its mission. In 2021, the FDIC awarded 483 contracts totaling over $2 billion for the acquisition of products and services. Many types of vendors, contractors, and subcontractors deliver these products and services to the FDIC. The supply chain for each vendor, contractor, or subcontractor may present unique risks to the FDIC, including the installation of counterfeit hardware and software into the FDIC environment, or the reliance on a malicious or unqualified provider. Further, the Agency may have reduced visibility, understanding, and control of these risks when its vendors rely on second- and third-tier suppliers and service providers. According to the National Institute of Standards and Technology (NIST), "adversaries are using the supply chain as an attack vector and [as an] effective means of penetrating [United States' public and private] systems, compromising the integrity of system elements, and gaining access to critical assets."[1]

Weaknesses in the FDIC's supply chains can compromise technology and the data stored on it, providing adversaries a means by which to inappropriately access or collect sensitive information.[2] Adversaries may seek to disrupt the FDIC's operations, programs, and functions and may manipulate or exploit its sensitive information for their own purpose or benefit. Therefore, the FDIC must implement a robust Supply Chain Risk Management (SCRM) Program to identify and mitigate supply chain risks that threaten its ability to fulfill its mission, goals, and objectives and protect sensitive information.

As reported by the U.S. Government Accountability Office (GAO), threat actors who exploit supply chain vulnerabilities could potentially compromise the confidentiality, integrity, or availability of an agency's systems and the information they contain.[3] As an example, in December 2020, Federal agencies experienced a supply chain cybersecurity event involving the network services provider SolarWinds. Attackers infiltrated SolarWinds' supply chain and inserted malicious code that created backdoor access into the product.

---

[1] NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations* (December 2018).
[2] FDIC Charter, *Supply Chain Risk Management Implementation Project* (November 2019).
[3] GAO Report, *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks* (GAO-21-171) (December 2020).

As customers, including multiple Federal agencies, downloaded installation packages from Solar Winds, attackers were able to access the Government network systems running the products. In response, the Department of Homeland Security issued an Emergency Directive stating that SolarWinds products "are currently being exploited by malicious actors. Disconnecting affected devices . . . is the only known mitigation measure currently available."

This cybersecurity event affected the FDIC, because it uses the SolarWinds product on its network. However, the FDIC stated that it implemented actions in accordance with Cybersecurity and Infrastructure Security Agency guidance to mitigate the effects of the SolarWinds cybersecurity event.[4]

The FDIC should take into consideration supply chain risks in order to keep FDIC information, assets, and personnel safe and secure.[5] Risks are realized when adversaries exploit existing supply chain vulnerabilities, though it may take years for such exploitation to occur or for an agency to discover the exploitation.

Our evaluation objective was to determine whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's goals and best practices. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Appendix 1 presents our evaluation objective, scope, and methodology.

BACKGROUND

According to the Office of Management and Budget, a supply chain is the linked set of resources and processes between multiple tiers of organizations that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services.[6] An SCRM Program is the process of identifying, assessing, and managing the risks associated with product and service supply chains. Identifying and managing supply chain risk is a complex undertaking due to the global and distributed nature of vendor supply chains and the limited amount of information about them.

[4] The Cybersecurity and infrastructure Security Agency is a U.S. Federal agency under the Department of Homeland Security. It leads the effort to understand, manage, and reduce risk to the Nation's cyber and physical infrastructure.
[5] OIG Report, *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (February 2021).
[6] Office of Management and Budget Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).

According to the FDIC, identifying and managing supply chain risk requires a coordinated effort across FDIC Divisions and Offices.[7] The FDIC seeks to identify vulnerabilities and threats throughout its supply chain and develop and implement strategies and controls to monitor and manage the associated risks.

Over the past several years, three Executive Orders highlight the importance of global supply chains to the U.S. economy and national security:

- Executive Order 13806 (July 21, 2017) emphasizes that resilient supply chains are essential to the economic strength and national security of the U.S.[8]
- Executive Order 14017 (February 24, 2021) states that the U.S. needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security.[9]
- Executive Order 14028 (May 12, 2021) includes actions to enhance software supply chain security.[10] The Order states that the "Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software."

The Federal Government has also issued a series of guidance documents related to SCRM:

- The Office of Management and Budget (OMB) issued Circular A-130, *Managing Information as a Strategic Resource.*[11]
- NIST has issued Special Publications (SP) 800-37 Revision 2, 800-161, and 800-53 Revision 5.[12]

The FDIC has also issued its own SCRM policies and guidance. In July 2019, the FDIC Chief Information Officer Organization (CIOO) issued policy number 19-006,

---

[7] FDIC Directive, *Supply Chain Risk Management Program,* No. 3720-01 (June 2021).
[8] Executive Order No. 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (2017).
[9] Executive Order No. 14017, *Executive Order on America's Supply Chains* (2021). The FDIC has determined that Executive Orders No. 13806 and No. 14017 are non-binding to the FDIC. They are included in this report because they provide context to the overall Federal Government approach to supply chain risk management.
[10] Executive Order No. 14028, *Executive Order on Improving the Nation's Cybersecurity* (2021).
[11] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016) (OMB Circular A-130). This Circular requires Federal agencies to implement SCRM principles. The FDIC has determined that OMB Circular A-130 is "generally applicable" to the FDIC, to the extent that the Circular aligns with OMB's statutory authorities, does not impose obligations on the FDIC based on statutes that are legally inapplicable to the FDIC, and does not conflict with the FDIC's independence, statutory obligations, or regulatory authority.
[12] NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations* (December 2018); NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020); and NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015). The FDIC has opined that NIST Special Publications contain statements of best practices or guidance, but the FDIC does not consider them as binding.

Policy on Supply Chain Risk Management, to establish a "supply chain risk management process for the procurement related activities of the CIOO." In December 2021, the CIOO rescinded this policy.

In addition, in November 2019, the FDIC established a Charter for the *Supply Chain Risk Management Implementation Project* (SCRM Implementation Project Charter). The Agency's goal, as stated in the SCRM Implementation Project Charter, was "to ensure continuous mission delivery and protect sensitive information by building a supply chain risk-aware culture and establish a risk management framework and governance." The Charter set out the following objectives:

- Identify authorities that impose SCRM requirements and others that should be implemented for good business practices and other reasons, such as mitigating reputational risk;
- Identify and document a clear and common understanding of known risks to products, services, or other contractual agreements that can be managed and prioritized for mitigation purposes;
- Increase corporate awareness of supply chain risk;
- Establish controls and identify tools that can be implemented in the near term that mitigate the highest priority supply chain risks; and
- Provide longer-term recommendations regarding an SCRM Program based on best practices that includes:
    - A risk management framework that is integrated into appropriate processes and allows for evaluating the impact of a risk on the FDIC, the likelihood of the risk materializing, the FDIC's preparedness to deal with that specific risk, and a tolerance threshold that reflects the FDIC's risk appetite; and
    - Continuous monitoring and evaluation of supply chain risk based on agreed-upon metrics and indicators.

The SCRM Implementation Project was governed by a Steering Committee, coordinated by a Project Manager, and carried out by a Working Group (SCRM Implementation Project team).[13]

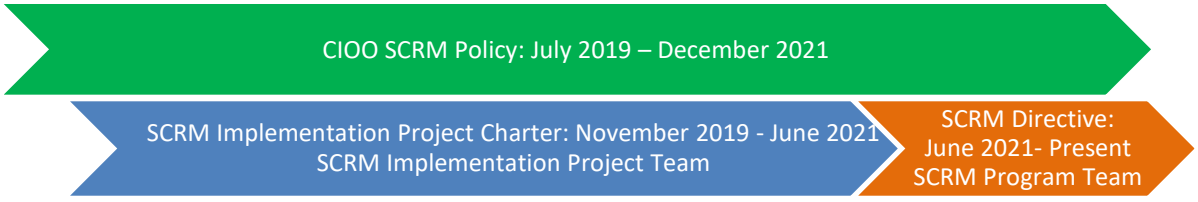
In June 2021, the FDIC issued Directive 3720.01 (SCRM Directive), establishing policy and responsibilities for the SCRM Program, pertaining to all FDIC Divisions

[13] The Steering Committee consisted of the Assistant General Counsel of the Legal Division's Legal Operations Section, Associate Director of the Division of Resolutions and Receiverships' Receivership Operations Branch, Chief Information Security Officer, Chief Risk Officer, Deputy Director of the Division of Administration's Acquisition Services Branch, Director of the Division of Information Technology's Chief Information Officer Organization, and the Special Advisor to the Chief Operating Officer.

and Offices. The SCRM Directive states that "[the] FDIC's goal is to manage its supply chain in a risk-based manner that allows it to fulfill its mission, goals, and objectives while protecting its sensitive and nonpublic information, and the integrity of its operations." The SCRM Directive designates the Chief Financial Officer as the Senior Accountable Official for SCRM, and it outlines the development of an SCRM Program Team to oversee the Division and Office efforts to "ensure consistent management of supply chain risks across the FDIC." The SCRM Directive also charges the FDIC Chief Risk Officer with managing the "development, dissemination, and maintenance of SCRM policy and procedures." The FDIC's SCRM Program is still in the initial stages of development and implementation.

The following graphic provides a timeline of the FDIC's efforts to develop policy related to SCRM:

Timeline of the FDIC's Policy Efforts Pertaining to SCRM



Source: OIG Analysis of FDIC CIOO SCRM Policy, SCRM Implementation Project Charter, and SCRM Directive.

EVALUATION RESULTS

The FDIC Must Identify, Evaluate, and Monitor Supply Chain Risks

We found that the FDIC has not implemented several objectives established in the SCRM Implementation Project Charter. Specifically, the FDIC has not:

- Identified and documented known risks to the FDIC's supply chain;
- Defined a risk management framework to evaluate risks to FDIC non-information technology (IT) procurements; and
- Established metrics and indicators related to continuous monitoring and evaluation of supply chain risks.

The FDIC must continue its efforts to fulfill its SCRM Implementation Project Charter objectives to identify, evaluate, and monitor supply chain risks. FDIC officials

acknowledged that the Agency is still in the process of implementing its SCRM Program and that progress against these objectives is ongoing.

The FDIC Has Not Identified and Documented Its SCRM Risks

The FDIC has not identified and documented a clear and common understanding of known risks to products, services, or other contractual agreements that can be managed and prioritized for mitigation.

The SCRM Implementation Project Steering Committee adopted the threat scenarios reported by the Cybersecurity and Infrastructure Security Agency (CISA) Information and Communication Technology (ICT) SCRM Task Force.[14] The CISA ICT SCRM Task Force report categorized the supply chain threats facing Federal agencies.[15] The Task Force report outlined 9 threat categories and 31 threat scenarios that impact Federal agencies, such as ransomware, counterfeit parts, and the inherited risks associated with extended supply chains.[16] See Appendix 2 of this report for details on the CISA ICT threat categories and threat scenarios.

However, the FDIC has yet to align these threat scenarios to the FDIC's SCRM Program by identifying those risks included in the Task Force report that pertain to the FDIC. An Implementation Team official stated that the processes and tools necessary to identify the FDIC-specific supply chain risks and threat scenarios were not yet in place. The official also stated that the FDIC's SCRM Steering Committee concluded that the SCRM Program Team would make these determinations. Once these processes and tools are in place, the FDIC should identify and document risks to its supply chain.

[14] In October 2018, CISA launched the SCRM Task Force, a public-private partnership to provide advice and recommendations to CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain. The Threat Evaluation Working Group was established for the purpose of the identification of processes and criteria for threat-based evaluation of ICT suppliers, products, and services. In January 2021, the Threat Evaluation Working Group issued its latest report titled *Threat Evaluation Working Group: Threat Scenarios Version 2.0* (January 2021).

[15] The SCRM Implementation Project Steering Committee adopted these threat scenarios because it determined that the nature of the supply chain threats the FDIC faces are similar to those faced by other Federal Government organizations.

[16] According to the *Threat Evaluation Working Group: Threat Scenarios Version 2.0* report, Inherited Risk (extended supplier chain) is defined as the threats that result from current supply chains that extend broadly across industries and geographies. These threats are typically associated with the challenge of extending controls and best practices through the entire supply chain due to its global nature. Inherited Risk also includes the vulnerabilities that can result from integration of components, products, or services from lower-tier suppliers.

Risk Management Framework Not Applied to Non-IT Procurements

The Implementation Project Team recommended a risk management framework, as required by the SCRM Implementation Project Charter, but its recommendation did not address non-IT procurements. The SCRM Directive states that the FDIC's SCRM Program is designed to identify and manage both IT and non-IT supply chain risks.[17]

When developing the SCRM Directive, the Implementation Project Team included a policy statement that the FDIC will apply the NIST Risk Management Framework (RMF).[18] However, the SCRM Directive states that the NIST RMF will be applied only to IT systems, products, and services. Therefore, the FDIC's SCRM Program has not identified a risk management framework for non-IT purchases. Absent a framework to assess the FDIC's non-IT supply chain risks, the FDIC may not effectively determine the likelihood or impact of these risks, such as a disruption in delivery of critical services or the decreased quality of the goods and services it purchases.

Risk Management Framework Not Implemented

CIOO officials stated that they are implementing the NIST RMF and related controls but have not yet integrated the NIST RMF into CIOO processes. The CIOO also has not tailored the NIST RMF to evaluate the impact of supply chain risks on the FDIC, the likelihood of those risks materializing, or the FDIC's preparedness to respond to those risks. The CIOO should continue its efforts to implement the NIST RMF, so that the FDIC can effectively identify and manage the IT-related supply chain risks to its systems, such as their susceptibility to the insertion of counterfeit components or software. Our reports on the FDIC's information security program in both 2020 and 2021 each contained a recommendation for the FDIC's CIOO to implement aspects of the NIST RMF. Our OIG report, *The FDIC's Information Security Program–2020* (October 2020), recommended that the CIOO ensure that all outsourced information systems are subject to the NIST RMF. Our OIG report, *The FDIC's Information Security Program–2021* (October 2021), recommended that the CIOO ensure that in-

[17] FDIC Directive 3720.01, *Supply Chain Risk Management Program* (June 2021).
[18] NIST SP 800-37, Revision 2 *Risk Management Framework for Information Systems and Organizations* (December 2018). The NIST RMF outlines controls related to gaining a clear understanding of the threats, vulnerabilities, and potential impacts of an adverse supply chain event. According to NIST, the RMF is purposefully designed to be technology neutral so that the methodology can be applied to any type of information system without modification. It also states that senior officials within the organization should ensure integration of SCRM considerations into planning/budgeting cycles, architectures, and acquisitions.

house and contractor-managed information systems are subject to a formal authorization process defined in the NIST RMF. Both recommendations remained unimplemented as of February 2022.

Metrics and Indicators Not Established

The NIST RMF recommends developing and implementing an organization-wide continuous monitoring strategy that can include supply chain risk considerations. The NIST RMF defines a continuous monitoring program as a program established to collect information in accordance with pre-established metrics, utilizing information readily available.

However, the FDIC has not established metrics nor indicators related to the continuous monitoring and evaluation of supply chain risks. If the FDIC does not identify, evaluate, and monitor supply chain risks, it may be exposed to SCRM threats such as the insertion of counterfeit components or malicious code. These threats could compromise the FDIC's technology and data and provide adversaries a means through people and products to inappropriately collect sensitive information such as confidential bank examination information. Absent efforts to monitor and evaluate supply chain risk, supply chain disruptions could compromise the products, services, and facilities that enable the FDIC to perform its mission.

As noted in our OIG report, *The FDIC's Information Security Program-2021* (October 2021), the FDIC has not defined processes and procedures that support the underlying components of the SCRM Directive. For example, we found that the FDIC did not have procedures that defined:

- How to implement its SCRM policy or strategy and associated baseline SCRM controls;
- Obtaining assurance over external service providers' compliance with the FDIC's cybersecurity requirements, including:
    - How to identify and prioritize externally provided systems, components, and services;
    - The organizational requirements for cybersecurity and SCRM for externally provided systems, system components, and services;
    - The tools or methods used to validate that SCRM requirements are being met;
    - The risk-based processes for evaluating SCRM risks associated with suppliers;
    - How awareness is maintained over risks stemming from upstream suppliers through monitoring activities; and

    - The integration of its acquisition process and the use of contractual stipulations detailing appropriate SCRM measures for external providers.
- Management of counterfeit components, including:
    - How to detect and prevent counterfeit components;
    - How to maintain configuration control over components being repaired or serviced; and
    - The process for reporting counterfeit components.

Without these SCRM processes and procedures, the FDIC cannot be assured that it will accurately identify and monitor its supply chain risks.

Recommendations

We recommend that the FDIC Senior Accountable Official for SCRM (Deputy to the Chairman and Chief Financial Officer):

1. Identify and document supply chain risks and threats the FDIC faces when purchasing goods and services.

2. Establish and implement a risk management framework for non-IT procurements that is integrated with the FDIC's procurement processes.

3. Establish and implement metrics and indicators to continuously monitor and evaluate supply chain risks at the FDIC.

We recommend that the Chief Information Security Officer:

4. Implement SCRM controls of the NIST RMF for IT procurements.

The FDIC Should Conduct Supply Chain Risk Assessments to Identify Vulnerabilities

Risk assessments provide increased understanding and visibility into the supply chain and associated risks. Supply chain risk assessments should identify various aspects of the supply chain vulnerabilities related to suppliers and sub-contractors, component parts and materials, country of origin, third-party suppliers, and officials of vendor organizations and sub-suppliers.

Based upon our research, we conclude that the FDIC should conduct supply chain risk assessments during the procurement process as a management best practice. OMB Circular A-130 requires agencies to "analyze risks (including supply chain

risks) associated with potential contractors and the products and services they provide." Additionally, NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* (December 2018), includes guidance for performing supply chain risk assessments. For example, NIST recommends that organizations conduct a system-level risk assessment during the "Prepare" step of the RMF (Task P-14: *Risk Assessment-System).* This recommended task envisions that supply chain risk assessments consider "vulnerabilities which may arise related to the disposition of a system or system element and from the use of external providers."

We met with officials from four Federal agencies, including an SCRM Program Director and procurement officials, that were beginning to conduct, or had established mature processes for conducting, supply chain risk assessments. Officials at all four agencies communicated that supply chain risk assessments provide useful information in developing SCRM procedures and processes.

The GAO found that the most widely implemented SCRM foundational practice implemented by Federal agencies was to establish a process to conduct a supply chain risk assessment of a potential supplier. In December 2020, the GAO reported on the progress of 23 Federal agencies in implementing ICT SCRM programs.[19] In its report, the GAO identified seven foundational practices based upon NIST and OMB guidance. These practices provide an organization-wide approach to ICT SCRM. The GAO compared these foundational practices to agency policies, procedures, and other documentation. The seven foundational practices are:

1. Establishing executive oversight of ICT activities, including designating responsibility for leading agency-wide SCRM activities;
2. Developing an agency-wide ICT SCRM strategy for providing the organizational context in which risk-based decisions will be made;
3. Establishing an approach to identify and document agency ICT supply chain(s);
4. Establishing a process to conduct agency-wide assessments of ICT supply chain risks that identify, aggregate, and prioritize ICT supply chain risks that are present across the organization;
5. Establishing a process to conduct a SCRM review of a potential supplier that may include reviews of the processes used by suppliers to design, develop, test, implement, verify, deliver, and support ICT products and services;

[19] GAO Report, *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks* (GAO-21-171) (December 2020).

6. Developing organizational ICT SCRM requirements for suppliers to ensure that suppliers are adequately addressing risks associated with ICT products and services; and
7. Developing organizational procedures to detect counterfeit and compromised ICT products prior to their deployment.

The FDIC SCRM Directive established the FDIC's SCRM Program. According to the Directive, it is the FDIC's policy to "identify vulnerabilities and threats throughout its supply chain and develop and implement strategies and controls to monitor and manage associated risks." The FDIC's SCRM Directive requires Division and Office Directors to identify and manage supply chain risks facing their Division or Office activities. The SCRM Directive also includes a number of policy statements outlining what the program is designed to do, including:

- Identify and manage supply chain risks associated with both IT and non-IT systems, products, and services; and
- Identify and manage supply chain risks in a manner that reflects the FDIC's risk appetite; risk tolerances; business needs; financial considerations; and the nature, sensitivity, urgency, and criticality of the acquisition.

We found that the FDIC is not conducting supply chain risk assessments during the procurement processes for the CIOO nor other Division and Office contracts. The FDIC's SCRM risk mitigation efforts have included issuing three Procurement Administrative Bulletins (PAB) and responding to cybersecurity incidents when they occur.[20] Our recent OIG report, *The FDIC's Information Security Program-2021* (October 2021), stated that while Federal agencies are required to develop and implement plans and strategies to assess and monitor their supply chain risks, the FDIC has not yet defined processes and procedures to accomplish these tasks.

In addition, in our OIG report, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (January 2022), we noted that the FDIC may use threat information to mitigate supply chain risks in FDIC procurements, among other activities.

[20] The FDIC issued three PABs relating to SCRM. In September 2020 and April 2021, the FDIC issued two PABs requiring the inclusion of SCRM-related provisions and clauses in new solicitations and contract awards, prohibiting the purchase of goods and services from certain companies. In December 2020, the FDIC issued one PAB prohibiting the use of purchase cards to procure information technology hardware, software, and services developed by certain companies.

However, the FDIC has not established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information. Supply chain risk assessments would provide the FDIC with an ability to identify and mitigate risks.

While the CIOO SCRM policy (19-006) required and OMB Circular A-130 currently requires supplier assessments for IT procurements, CIOO officials stated that the organization does not currently have a process to complete such assessments. The CIOO policy required the CIOO to conduct a supplier assessment prior to entering into a contract for systems, system components, or software services; however, in December 2021, the CIOO rescinded this policy.

According to CIOO officials, they intended to conduct supplier assessments as part of the CIOO's Outsourced Solution Assessment Methodology (OSAM) process. However, the CIOO stopped using the OSAM process in the summer of 2020 and adopted the NIST RMF.[21] Our recent OIG report, *The FDIC's Information Security Program – 2021*, also identified that the CIOO had stopped using the OSAM process and that the CIOO had not conducted proper security risk assessments over certain systems.

In 2019, the CIOO started to develop a Standard Operating Procedure to describe the scope, the business rules, and the roles and responsibilities for identifying, reviewing, assigning, and reporting on supply chain risks in accordance with NIST and FDIC policy. However, CIOO officials stated that this Standard Operating Procedure will not be finalized because the FDIC has issued the SCRM Directive to provide enterprise-wide policy to manage SCRM risk.

Although it has been over 2 years since the FDIC first developed its SCRM Implementation Project Charter and CIOO policy, the FDIC has not established and maintained processes for conducting supply chain risk assessments, and the SCRM Program is still in its initial stages. FDIC officials stated that they are in the process of evaluating existing processes and tools to determine whether they adequately address the specific supply chain risks facing the FDIC.

Visibility into supply chain activities is important for monitoring and identifying high-risk events. If malicious actors are able to exploit vulnerabilities in the FDIC's supply chain, they could cause serious adverse impacts on the Agency's mission, operations, assets, and employees.

[21] The FDIC used OSAM to provide a consistent, well-informed, and ongoing security process for outsourced information systems and services.

Because the FDIC is a financial regulator and holds vast amounts of sensitive and nonpublic information, adversaries may seek to disrupt the Agency's operations, programs, and functions or seek to manipulate and exploit its sensitive information for their own purpose or benefit. According to the FDIC's November 2021 *Monthly APS Awards Summary Report*, in 2021, the FDIC awarded 483 contracts totaling over $2 billion.[22] Without increased visibility into its supply chains and the associated risks, it is difficult for the FDIC to manage those risks and reduce its susceptibility to adverse events.

Recommendations

We recommend that the FDIC Senior Accountable Official for SCRM (Deputy to the Chairman and Chief Financial Officer) in cooperation with the Deputy to the Chairman, Chief Operating Officer, and Director, Division of Administration:

5. Develop and implement a process and procedures for conducting supply chain risk assessments.

6. Conduct supply chain risk assessments prior to entering into contracts with new suppliers/vendors.

7. Conduct supply chain risk assessments prior to substantive contract actions, including renewals, extensions, and exercising option periods.

The FDIC Should Fully Capture SCRM Risks in Its Enterprise Risk Processes

FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program* (ERM Directive) (October 2018), establishes FDIC policy, responsibilities, and key components for the FDIC's Enterprise Risk Management (ERM) Program. The FDIC's ERM Program seeks to identify, assess, and address risks (including emerging risks) that could adversely impact the Agency's ability to achieve its goals, objectives, and mission. One of the objectives of the program is to increase awareness of emerging risks and provide opportunities to address them before they occur. The FDIC's ERM Program components include the use of a Risk Inventory and Risk Profile.

[22] The acronym "APS" is an abbreviation for Automated Procurement System.

The FDIC's Risk Inventory is a detailed list of risks that could affect the FDIC's ability to meet its strategic objectives. FDIC Divisions and Offices identify the risks and provide an assessment of their potential impact and likelihood. The ERM Directive states that the Risk Inventory should be updated as the FDIC identifies new risks or as risks change. The Risk Inventory items are prioritized and summarized in the FDIC's Risk Profile. The purpose of the FDIC's Risk Profile is to provide an analysis of the risks the FDIC faces both as it seeks to achieve its strategic objectives and arising from its activities and operations.[23] It lists the most significant risks identified through the risk assessment process and is not intended to be a complete inventory of all risks.

We found that the FDIC had not integrated Agency-wide supply chain risks into its ERM processes, even though it has identified certain potential threats related to SCRM risks, such as exposure to theft of intellectual property and the compromise of sensitive information. The FDIC's SCRM Directive states that "[t]he FDIC relies on a variety of products, systems, and services from external providers to fulfill its mission. These resources include both IT (e.g., computer systems, telecommunications equipment, software applications) and non-IT resources (e.g., office supplies, construction services, health and safety equipment, and consulting services)." The FDIC's SCRM Directive further states that "any broken link in the supply chain can adversely affect the FDIC's work" and that the FDIC must "consider supply chain risks … from a corporate-wide perspective, taking into account the overall strategic goals and objectives of the FDIC in carrying out its mission and business functions."

While the FDIC has established that supply chain risks can adversely impact its operations and mission, it has not addressed SCRM risks within its ERM Program from an Agency-wide perspective. The FDIC's CIOO has included an entry on SCRM to the FDIC Risk Inventory since October 2019. However, the CIOO's SCRM Risk Inventory entry is limited to the integrity of the CIOO's ICT products and services supply chain.

None of the other FDIC Divisions or Offices (besides the CIOO) reported supply chain risk items in the FDIC Risk Inventory for the enterprise. As a result, the FDIC's Risk Inventory does not capture all of the supply chain risks that other FDIC Divisions and Offices face, nor does it capture supply chain risks related to non-IT products and services.

[23] The Risk Profile captures the aggregate level and types of risk that the FDIC is willing to assume. The FDIC Chief Risk Officer, together with the Division of Finance and the Office of Risk Management and Internal Controls, maintain the Risk Profile.

For example, we recently reported that the FDIC's Division of Administration has primary responsibility for managing critical building services at all FDIC-owned facilities and for overseeing the operation, maintenance, repair, and replacement of mechanical equipment, parts, and systems that support a wide range of building services. [24] Threats to the uninterrupted delivery of these vital services can come from numerous sources, including the FDIC's supply chain, and were not reported in the FDIC's Risk Inventory.

An official within the FDIC's Office of Risk Management and Internal Controls stated that the Risk Profile entry discussing contract oversight touches on SCRM and discusses some supply chain risks. However, the Risk Inventory entries supporting this Risk Profile do not address supply chain risks.

According to the FDIC's ERM Directive, if risks are not effectively identified, assessed, and addressed, they could negatively affect the FDIC's ability to achieve its goals and objectives. The ability to address risks is critically important for the FDIC to fulfill its mission amid existing and emerging challenges.

Recommendation

We recommend that the Senior Accountable Official for SCRM (Deputy to the Chairman and Chief Financial Officer):

8. Ensure that the FDIC's Risk Inventory and Risk Profile clearly articulate the extent and significance of supply chain risks that face the FDIC.

The FDIC Should Properly Maintain Contract Documents

On September 3, 2020 and April 5, 2021, the FDIC issued two Procurement Administrative Bulletins requiring FDIC Contracting Officers to include new SCRM provisions and clauses in contracts awarded or modified after these dates.[25] The SCRM provisions and clauses prohibit contracting for hardware, software, and services developed or provided by certain, specified companies.[26] While Contracting

[24] OIG Report, *Security of Critical Building Services at FDIC-owned Facilities* (AUD-21-003) (March 2021). Critical building services include electrical power; heating, ventilation, air conditioning; and water.
[25] On June 1, 2022, the OIG corrected the dates of these two Procurement Administrative Bulletins. The prior version of the report listed them as being issued on September 5, 2020 and April 3, 2021.
[25] According to the FDIC's *Acquisition Procedures, Guidance, and Information*, the specified companies are: Kaspersky Lab, Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company.

Officers included these new provisions and clauses in contracts, we found that Contracting Officers did not maintain contract documents, as required.

The accuracy and completeness of file documentation to support contracting decisions is an essential element of contract administration. The FDIC's *Acquisition Procedures, Guidance, and Information* (PGI) requires the Contracting Officer to upload the contract into the Contract Electronic File (CEFile) system.[27] The Contracting Officer must also provide CEFile access to the designated Oversight Manager and any designated Technical Monitors so they can view the contract and maintain their Oversight Manager file.[28]

Contracting Officers did not maintain contract documents in the CEFile system. Two of the five contracts we reviewed were not stored in the CEFile system (both were subsequently provided to the OIG). We have included contract oversight as a Top Management and Performance Challenge facing the FDIC since 2017. In October 2019, we reported a similar finding pertaining to contract oversight documentation that was not properly stored in CEFile.[29] In response to our findings from 2019, the FDIC established a routine process to perform internal reviews to verify that Oversight Managers upload documents into the contract document system in a timely manner and maintain complete files. Given the persistent issues with maintaining contract documentation, it appears that the control established in response to our report in October 2019 does not adequately ensure that contract files contain required documents.

Our OIG report *Contract Oversight Management* (October 2019), noted that Oversight Managers did not upload contract-related documentation due to the challenges associated with system faults and the amount of time required to upload documentation. Contracting personnel stated that CEFile was "not user-friendly" and described the system as being time-consuming and burdensome. In response to that report, the FDIC stated that it was working to replace the current system with a new "end-to-end procurement system." However, nearly 2 years later, the FDIC has not implemented a new system.

As noted in our prior report, the omission of critical documents in CEFile could lead to difficulty in enforcing a contract in the event of contractor noncompliance. Also,

[27] The PGI contains procedures for implementing the FDIC's Acquisition Policy Manual.
[28] Oversight Managers (OM) are responsible for ensuring contractors deliver required goods or perform work according to the contracts and delivery schedules. OMs also monitor the expenditure of funds in relation to contract dollar ceilings and approve invoices. For complex contracts, the OM may nominate one or more Technical Monitors to assist the OM in carrying out contract oversight responsibilities.
[29] OIG Report, *Contract Oversight Management* (EVAL-20-001) (October 2019).

when contract documents are not timely uploaded to CEFile, the FDIC has limited assurance of a smooth transition of contract oversight when Contracting Officers are reassigned or leave the Agency.

Recommendation

We recommend that the Deputy to the Chairman, Chief Operating Officer, and Director, Division of Administration:

9. Implement internal controls to ensure that Contracting Officers maintain contract documents in the FDIC's acquisition system as required, and are held accountable for failure to do so.

FDIC COMMENTS AND OIG EVALUATION

On February 25, 2022, FDIC Management provided a written response to a draft of this report. The FDIC response is presented in its entirety in Appendix 4. In its response, FDIC Management stated that the SCRM Team continues to implement the SCRM Program objectives and is working to expand its Agency-wide SCRM guidance.

In its response, FDIC Management identified certain processes and controls, which, in its view, help to mitigate supply chain risks. Our evaluation objective was to determine whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's goals and best practices. Therefore, we assessed whether the FDIC was achieving its own goals and whether its processes were in accordance with best practices. Our evaluation of the SCRM Program did not assess all processes and controls within the FDIC environment, as that would have been beyond the scope of this evaluation. The FDIC also took certain actions referenced in its management response after we had previously shared a draft of this report. Because the FDIC took these actions shortly before issuance of the report, they were not within the scope of our fieldwork. Therefore, we have not reviewed the actions to determine whether they will be implemented effectively at the FDIC or in accordance with best practices.

In its response, FDIC Management concurred with all nine recommendations in our report. FDIC Management proposed corrective actions that were sufficient to address the nine recommendations. Therefore, we consider these nine recommendations to be resolved. The recommendations will remain open until we confirm that corrective actions have been implemented and are satisfied that the actions are responsive. A summary of the FDIC's corrective actions is contained in Appendix 5.

Objective

The evaluation objective was to determine whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's goals and best practices.

We conducted this evaluation from July 2021 through October 2021 in accordance with the Council of Inspectors General on Integrity and Efficiency *Quality Standards for Inspection and Evaluation* (issued January 2012).[30]

Scope and Methodology

The scope of our evaluation focused on the FDIC's efforts to develop and implement its SCRM Program. To obtain an understanding of the FDIC's efforts to develop and implement its SCRM Program, we interviewed FDIC officials and staff from the Division of Administration, the Chief Financial Officer Organization, and the Chief Information Officer Organization and reviewed the following relevant FDIC policies, and documents:

- The FDIC CIOO's *Policy on Supply Chain Risk Management*, number 19-006 (July 2019);
- The FDIC Charter, *Supply Chain Risk Management Implementation Project* (November 2019);
- FDIC Directive *Supply Chain Risk Management Program,* number 3720-01 (June 2021);
- The FDIC *SCRM Team Charter* (October 2021);
- The SCRM Implementation Team's Implementation Project Plan and accompanying documents;
- The FDIC Risk Inventory and Risk Profile documents issued June through October 2021; and
- FDIC *Enterprise Risk Management and Internal Control Program* Directive (October 2018).

To develop criteria for assessing the FDIC's efforts, we used the CIOO SCRM Policy, the FDIC's SCRM Implementation Project Charter, and the FDIC's SCRM Directive. We supplemented the FDIC's internal documents with the following additional criteria:

[30] In December 2020 the Council of Inspectors General on Integrity and Efficiency issued an update to the *Quality Standards for Inspection and Evaluation* which is effective for all inspections and evaluations beginning on or after January 1, 2022. Because we initiated this evaluation in July 2021, we adhered to the January 2012 standards.

- Government-wide policy, including:
  - Executive Order No. 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (July 21, 2017) and the resulting report, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (September 2018);
  - Executive Order No. 14017, *Executive Order on America's Supply Chains* (February 24, 2021) and the resulting report, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth* (June 2021); and
  - Presidential Executive Order No. 14028, *Executive Order on Improving the Nation's Cybersecurity* (May 12, 2021).

- NIST security standards and guidance, including:
  - NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations* (December 2018);
  - NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020); and
  - NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015).

- Reviewed the following OIG reports:
  - OIG Report, *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (2016, 2018, 2019, 2020, 2021);
  - OIG Report, *Contract Oversight Management* (EVAL-20-001, October 2019);
  - OIG Report, *The FDIC's Information Security Program-2020* (AUD-21-001) (October 2020);
  - OIG Report, *Security of Critical Building Services at FDIC-owned Facilities* (AUD-21-003) (March 2021);
  - OIG Report, *The FDIC's Information Security Program-2021* (AUD-22-001) (October 2021); and
  - OIG Report, *Sharing of Threat Information to Guide the Supervision of Financial Institutions* (AUD-22-003) (October 2021)

- We reviewed the GAO Report, *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* GAO-21-171 (December 2020) on Government Agencies' implementation of SCRM foundational practices.

- We reviewed Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource* (July 2016).

To develop the best practices used in this report, we interviewed officials and gathered information from four Federal agencies: the Defense Intelligence Agency, the Department of Homeland Security, the General Services Administration, and the National Aeronautics and Space Administration. We chose these agencies because they have, or are developing, SCRM Programs. Two agencies had more mature programs that have been functioning for several years. The other two agencies are still developing SCRM Programs and shared their planned approaches. We interviewed these officials to gain an understanding of lessons learned as they developed or carried out their SCRM Programs.

To ensure that the FDIC had included required SCRM-related provisions and clauses in FDIC contracts, we reviewed five contracts awarded after the effective date of the September 2020 PAB. We also interviewed Acquisition Services Branch staff to gain an overview of the process to develop, issue, and implement FDIC PABs.

Table 1 illustrates the supply chain threat categories and threat scenarios outlined in the CISA Threat Evaluation Working Group report *Threat Evaluation Working Group: Threat Scenarios Version 2.0*.

Table 1: Threat Categories and Threat Scenarios Identified in CISA Threat Evaluation Working Group Report

Threat Category	Threat Scenarios
Counterfeit Parts	• Counterfeit/Fraudulent Parts
External Attacks On Operations and Capabilities	• Attacker Exploits Known Vulnerabilities in Supplier Systems Connected to Critical Infrastructure Organization Networks • Incorrect Border Gateway Protocol Routing • Ransomware • Removal Media Attack • Resource Depletion
Internal Security Operations and Controls	• Poor Access Control Policy • Devices that Don't Auto-Update Firmware • Mishandling of Critical or Sensitive Information • Lack of Asset Visibility and Vulnerability Exploitation • ICT Devices with Default Passwords • Incorrect Privilege Settings, Authorized Privileged User, or Administrator Erroneously Assigns User Exceptional Privileges or Sets Privilege Requirements on a Resource Too Low
Compromise of System Development Life Cycle Processes and Tools	• Developmental Process of Hardware and Software
Insider Threats	• Contractor Compromise Scenario • New Vendor Onboarding • Staffing Firms Used to Source Human Capital • Contractor Compromise
Economic Risks	• Financial Strength of the Supplier • Information Asymmetries • Ownership Change • Cost Volatility
Inherited Risk (Extended Supplier Chain)	• Sub-agency Failure to Update Equipment • Sub-agency Failure to Update Enterprise Software • Inheriting Risk from Third Party Supplier • Mid-Supply Insertion of Counterfeit Parts Via Supplier XYZ to Trusted/Vetted Vendor
Legal Risks	• Laws that Harm or Undermine American Economic Interests • Legal Jurisdiction-Related Threats
External, End-To-End Supply Chain	• Natural Disasters/Pandemic Causing Supply Chain Disruptions • Man Made Disruptions: Sabotage, Terrorism, Crime, and War • Labor Issues • Influence or Control by Foreign Governments Over Suppliers

Source: *Threat Evaluation Working Group: Threat Scenarios Version 2.0* (January 2021).

Acronyms and Abbreviations

CEFile	Contract Electronic File
CIOO	Chief Information Officer Organization
CISA	Cybersecurity and Infrastructure Security Agency
ERM	Enterprise Risk Management
FDIC	Federal Deposit Insurance Corporation
GAO	Government Accountability Office
ICT	Information and Communication Technology
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OM	Oversight Manager
OMB	The Office of Management and Budget
OSAM	Outsourced Solution Assessment Methodology
PAB	Procurement Administrative Bulletin
PGI	Procedures, Guidance, and Information
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SP	Special Publication
TMPC	Top Management and Performance Challenge

Federal Deposit Insurance Corporation

Memo

TO: Terry L. Gibson
Assistant Inspector General for Audits, Evaluations, and Cyber

FROM: Bret D. Edwards BRET EDWARDS Digitally signed by BRET EDWARDS Date: 2022.02.25 16:28:18 -05'00'
Deputy to the Chairman and Chief Financial Officer

DATE: February 25, 2022

RE: Management Response to OIG Draft Evaluation Report, The FDIC's Implementation of Supply Chain Risk Management (No. 2021-013)

The FDIC has completed its review of the Office of Inspector General's (OIG) draft evaluation report titled *The FDIC's Implementation of Supply Chain Risk Management*, issued on January 26, 2022. FDIC management concurs with the report's nine recommendations, which are generally consistent with the Supply Chain Risk Management (SCRM) program implementation plans we shared with the OIG at the onset of the evaluation.

The FDIC has made, and continues to make, notable progress in implementing an effective agency wide SCRM program and has meaningful control practices in place to mitigate supply chain risk. The FDIC began building its SCRM program in earnest in November 2019 with the approval of the SCRM Implementation Project Charter. Importantly, this project was a discrete effort to launch the development of the FDIC's SCRM program. The FDIC assembled a cross-organizational SCRM Implementation Project team, which researched and identified SCRM requirements and related guidance, established an SCRM governance structure, and worked to raise SCRM awareness. The team's capstone achievement was the issuance of the FDIC's first corporate-wide SCRM Directive in June 2021. The Directive lays the foundation of FDIC's SCRM program; introduced elements of the Corporation's overall SCRM strategy; communicated associated policy, roles, and responsibilities; and defined the responsibilities of a more permanent, cross-organizational SCRM Team to develop and assist in the implementation of the FDIC's SCRM strategies, plans, processes, and controls. SCRM Implementation Project team members transitioned their work to a permanent cross-organizational SCRM Team in September 2021. The SCRM Team, a program element recommended by the National Institute of Standards and Technology (NIST), will further define and implement the SCRM program. The SCRM Team has met regularly since it was established and continues to implement SCRM program objectives transitioned from the SCRM Implementation Project team.

In addition, the FDIC has existing processes and controls that are already in place and are important in mitigating supply chain risk. These procedures and controls include:

- Using targeted Requests for Proposals (RFPs) to solicit proposals from reputable or trusted suppliers;
- Conducting risk-based background investigations of contractor personnel;
- Reviewing procurement packages to ensure inclusion of:
    - Required information security and privacy clauses and provisions, and

  - Descriptions of how the NIST Risk Management Framework (RMF) will be applied to the contracted systems or services.
- Obtaining approval from the Security and Enterprise Architecture Technical Advisory Board (SEATAB) before the introduction and use of new technology; and
- Conducting visual inspections of incoming packages containing IT hardware to:
  - Identify damage or evidence of tampering, and
  - Verify that the original seal from the vendor/manufacturer is intact.

The FDIC also requires that new or modified contracts include SCRM provisions that prohibit contracting for hardware, software, and services developed or provided by certain, specified companies.

The FDIC has also implemented the NIST RMF and integrated it into CIOO processes. Those processes are updated and refined as NIST periodically issues new requirements and guidance. In this regard, the FDIC is in the process of selecting appropriate security controls from the SCRM control family in NIST SP 800-53 and will apply those selected controls during IT procurement efforts. The FDIC has also implemented a process that subjects all acquisitions to a review to determine those that require authorization activities consistent with the RMF. Any acquisition requiring authorization is subject to the RMF process. More broadly, the FDIC adopted the RMF in June of 2020 and rescinded legacy approval processes. Since then, the FDIC has consistently applied the RMF to all new FDIC developments and deployments. Additionally, as the FDIC continues to mature processes relating to the system development lifecycle (SDLC), the CIOO adopted a new SDLC on January 13, 2022, which calls for project teams to consider the impact of the RMF in planning, developing, and delivering software solutions because RMF requirements help to ensure that security, privacy, and cyber-SCRM activities are addressed.

Additionally, regarding the statement in the draft evaluation report that references the rescission of CIOO SCRM Policy 19-006, it is important to note that the CIOO rescinded the policy in December 2021 to ensure that the CIOO's policy approach aligned with the SCRM Corporate-wide Directive and subsequent guidance. The cross-organizational SCRM Team is actively working to expand SCRM Corporate-wide guidance.

Finally, the OIG report concluded that the FDIC had not ensured that its ERM processes address non-IT supply chain risks. In addition to including specific SCRM risk items, the FDIC's ERM Risk Profile and Risk Inventory include risk items related to contract administration, which includes the risk of not having access to needed products, systems, or services or not having access to enough supplies or materials. These risk items address both IT and non-IT products and services.

Our specific responses to the evaluation findings and each recommendation follow.

Management Response to the OIG Recommendations

Recommendation 1: Identify and document supply chain risks and threats the FDIC faces when purchasing goods and services.

Management Decision: Concur.

Planned Action:

As stated in the report, the SCRM Implementation Project Steering Committee adopted the threat scenarios identified by the Cybersecurity and Infrastructure Security Agency (CISA) Information and Communication Technology SCRM Task Force.

Consistent with our implementation plan, the SCRM Team will next identify those CISA threat scenarios that are particularly applicable to the FDIC and consider whether there are additional program-level risks that the SCRM program should be designed to mitigate. The SCRM Team will document the results of that analysis.

Estimated Completion Date: June 30, 2022.

Recommendation 2: Establish and implement a risk management framework for non-IT procurements that is integrated with the FDIC's procurement processes.

Management Decision: Concur.

Planned Action:

As we discussed with OIG during the evaluation, the SCRM directive, issued in June 2021, provides the policy and roles and responsibilities framework for managing supply chain risks. The directive includes ten policy statements that comprise the framework for the FDIC's SCRM program. All but one policy statement applies to non-IT procurements. The Directive also assigns SCRM responsibilities to officials outside of the CIO Organization, including the CFO, CRO, Operating Committee, SCRM Team, COO, DOA, ASB Director, Division/Office officials, and individuals including oversight managers and purchasers of products, systems, or services.

The FDIC uses an ERM framework as described in our ERM Standard Operating Procedure, to identify, assess, respond to, and monitor all enterprise risks, both IT and non-IT. Our ERM framework is based on OMB Circular A-123 and the ERM Playbook. The FDIC has also implemented the NIST Risk Management Framework for information security and privacy risks, including SCRM IT-related risks.

Additionally, the FDIC has adopted the GAO's *Standards for Internal Control in the Federal Government* (Green Book) as the internal control framework for all FDIC programs and operations. NIST Special Publication 800-53, Revision 5 provides a catalog of information security and privacy controls, including controls intended to mitigate supply chain risk.

The FDIC's procurement program is subject to ERM risk assessment and DOA's Acquisition Services Branch has developed internal controls over procurement processes that are subject to internal review. Risks associated with individual procurements, including security and privacy risk, are considered during the acquisition planning process. As discussed in response to recommendations 5, 6, and 7, we will also implement a risk-based process for considering supply chain risk in individual procurement actions.

The FDIC is developing a written SCRM strategy document to implement the SCRM Directive. That document will reiterate that the SCRM Directive addresses both IT and non-IT supply chain risks, that our ERM framework and the Green Book provide the risk management and internal control frameworks for all programs and operations, and that the NIST RMF provides a more targeted control framework for information security and privacy risks.

Estimated Completion Date: June 30, 2022.

Recommendation 3: Establish and implement metrics and indicators to continuously monitor and evaluate supply chain risks at the FDIC.

Management Decision: Concur.

Planned Action:

As the FDIC continues to build out the SCRM program, the SCRM Team will develop meaningful metrics and indicators for gauging and monitoring supply chain risk.

Estimated Completion Date: September 30, 2022.

Recommendation 4: Implement SCRM controls of the NIST RMF for IT procurements.

Management Decision: Concur.

Planned Action:

The FDIC will select appropriate security controls from the SCRM control family in NIST SP 800-53, commensurate with risk, as part of the FDIC's implementation of the NIST RMF. FDIC will then apply those selected controls during IT procurement efforts.

Estimated Completion Date: October 31, 2022.

Recommendation 5: Develop and implement a process and procedures for conducting supply chain risk assessments.

Management Decision: Concur.

Planned Action:

Consistent with our SCRM implementation plan, the SCRM Team will draft procedures to implement the SCRM directive. This effort will include defining a risk-based process for considering supply chain risk in individual procurement actions. The FDIC will implement this process as part of the procurement process.

Estimated Completion Date: November 30, 2022.

Recommendation 6: Conduct supply chain risk assessments prior to entering into contracts with new suppliers/vendors.

Management Decision: Concur.

Planned Action:

The FDIC will apply the process discussed in response to Recommendation 5 in a risk-based manner when entering into new contracts.

Estimated Completion Date: November 30, 2022.

Recommendation 7: Conduct supply chain risk assessments prior to substantive contract actions, including renewals, extensions, and exercising option periods.

Management Decision: Concur.

Planned Action:

The FDIC will apply the process discussed in response to Recommendation 5 in a risk-based manner when contract option periods are exercised or contracts are renewed or extended. The FDIC will evaluate whether there are examples of other substantive contract actions that should be subject to supply chain risk assessment and will reflect such examples in SCRM procedures.

Estimated Completion Date: November 30, 2022.

Recommendation 8: Ensure that the FDIC's Risk Inventory and Risk Profile clearly articulate the extent and significance of supply chain risks that face the FDIC.

Management Decision: Concur.

Planned Action:

As discussed earlier, multiple risk inventory items address IT and non-IT SCRM risks. However, ORMIC will review the ERM Risk Inventory and Risk Profile to ensure clear and appropriate reflection of supply chain-related enterprise risks facing the FDIC.

Estimated Completion Date: March 31, 2022.

Recommendation 9: Implement internal controls to ensure that Contracting Officers maintain contract documents in the FDIC's acquisition system as required, and are held accountable for failure to do so.

Management Decision: Concur.

Planned Action:

The FDIC provided training to Contracting Officers in the second half of 2021 to emphasize the importance of existing controls for maintaining contract documents. DOA management will reemphasize contract documentation expectations. In addition, ORMIC will continue to coordinate contract reviews to verify, among other things, compliance with contract documentation requirements. ORMIC will provide review results to ASB for consideration in Contracting Officer performance management reviews.

Estimated Completion Date: June 30, 2022.

This table presents management's response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The FDIC will identify and document the CISA threat scenarios that are particularly applicable to the FDIC, consider whether there are additional program-level risks that the SCRM Program should be designed to mitigate, and document the results of its analysis.	June 30, 2022	$0	Yes	Open
2	The FDIC will develop and document a SCRM strategy to implement the SCRM Directive. The document will discuss risk-based processes and frameworks for considering supply chain risks in individual, IT and non-IT procurement actions.	June 30, 2022	$0	Yes	Open
3	The FDIC will develop meaningful metrics and indicators for gauging and monitoring supply chain risk.	September 30, 2022	$0	Yes	Open
4	The FDIC will select appropriate security controls from the SCRM control family in NIST guidance, as part of its implementation of the NIST RMF, and then apply those selected controls during IT procurements.	October 31, 2022	$0	Yes	Open
5	The FDIC will draft procedures to implement the SCRM Directive. This effort will define a risk-based process for considering supply chain risks in individual procurement actions.	November 30, 2022	$0	Yes	Open
6	The FDIC will apply the process described in response to recommendation 5 when entering into contracts with new suppliers/vendors.	November 30, 2022	$0	Yes	Open
7	The FDIC will apply the process described in response to recommendation 5 in a risk-based manner when contracts are renewed, extended, or have option periods exercised. The FDIC will evaluate whether other substantive contract actions should be subject to supply chain risk assessments.	November 30, 2022	$0	Yes	Open

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
8	The FDIC will review the ERM Risk Inventory and Risk Profile to ensure clear and appropriate reflection of supply-chain related enterprise risks.	March 31, 2022	$0	Yes	Open
9	The FDIC will reemphasize contract documentation expectations, continue to conduct contract reviews to verify compliance with contract documentation requirements, and coordinate the results for consideration in evaluating Contracting Officer performance.	June 30, 2022	$0	Yes	Open

[a] Recommendations are resolved when —

1. Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
2. Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
3. Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when the OIG confirms that corrective actions have been completed and are responsive.

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.